Hablemos de fortalecer la seguridad digital para la defensa del medio ambiente en Colombia

Fundación Karisma

<K+LAB>

En un esfuerzo para que todas las personas tengan acceso al conocimiento, la Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.

Bogotá, Colombia
Agosto, 2024

Autoras
Carolina Botero
Nicholas Güecha

Con apoyo de
Pilar Saénz
Angie Ballesteros

Talleristas
Lorena Enciso
Alejandra Zuñiga

Dirección Fundación Karisma
Catalina Moreno Arocha
Juan Diego Castañeda

Coordinación del Laboratorio de Seguridad y Privacidad Digital K+LAB
Carolina Botero

Coordinación Participación Cívica
Pilar Sáenz

Coordinación editorial
Natalia Andrade Fajardo

Diseño editorial
Daniela Moreno Ramírez

Contenido

Introducción

Global Witness en su informe de 2022[1] documentó los asesinatos de personas defensoras del medio ambiente en 18 países, 11 de ellos en América Latina. De este grupo, Colombia fue el país que registró el mayor número de homicidios, y además para ese año los había duplicado respecto de los contabilizados en 2021. Este informe confirma lo que ya sabíamos: la defensa del medio ambiente es una actividad muy riesgosa en nuestro país. A quienes realizan esta labor frecuentemente se les hostiga y amenaza, en ocasiones tales situaciones pueden materializarse poniendo en riesgo su integridad personal.

1. *https://www.globalwitness.org/es/standing-firm-es/*

Hoy en día estas situaciones también se dan en el entorno digital y, sin embargo, no sabemos mucho de esta problemática. En 2023 Fundación Karisma se acercó a diferentes organizaciones defensoras del medio ambiente en territorios en conflicto ambiental en Colombia para analizar de forma cercana y directa su situación de seguridad. Aunque el grupo no es estadísticamente representativo, sí permitió tener una primera aproximación para entender contextualmente sus prácticas y experiencias. En este documento se recoge el resultado del trabajo realizado con personas que hacen parte de seis organizaciones colombianas que operan en tres regiones periféricas de importancia ambiental en el país.

Con estas personas, Karisma comprobó que el uso de las tecnologías digitales e internet juegan un rol central en la defensa de los derechos humanos vinculados al medio ambiente. Las organizaciones aprovechan estas herramientas para fortalecer sus agendas de trabajo y conectarse con redes más

amplias. Sin embargo, el acoso, el hostigamiento, las amenazas y la vigilancia, que antes se limitaban a interacciones cara a cara o comunicaciones físicas, han encontrado nuevas formas de expresión en el mundo digital.

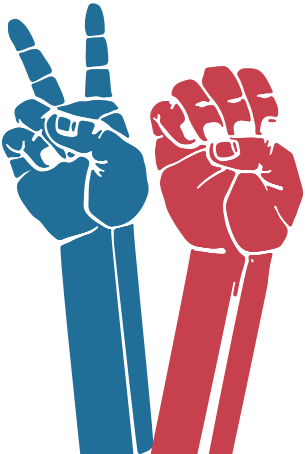
Lo que está pasando con las tecnologías amplifica el impacto de las amenazas que sufre esta población. Ahora bien, las amenazas digitales que enfrentan no se quedan en el espacio virtual, tienen consecuencias tangibles y directas en la vida cotidiana de las personas y se entrelazan con problemáticas preexistentes como el racismo, el sexismo y la desigualdad, agravando las condiciones de vulnerabilidad y el riesgo que enfrentan.

El documento empieza con una nota metodológica que explica brevemente las actividades que se hicieron para entender el contexto en el que las personas defensoras del medio ambiente hacen su activismo en territorios en disputa en Colombia. La segunda sección enuncia los tipos de amenazas

identificadas a partir de las mencionadas actividades, cada una va acompañada de una descripción del contexto en relación con las experiencias de esta población. La tercera parte consiste en un conjunto de recomendaciones mínimas que pueden mejorar la situación de seguridad digital de esta población.
El documento cierra con unas conclusiones y una propuesta de agenda con temas a profundizar; es una hoja de ruta para seguir explorando y creando mecanismos de mitigación de esta problemática.

Sabemos que la seguridad es un tema situado y contextual, es decir, que el análisis de riesgos varía según las condiciones particulares de las organizaciones -e incluso de cada persona- y que las acciones de mitigación hechas a la medida de cada uno son más efectivas. Sin embargo, como existe una población que comparte una serie de condiciones, su seguridad digital puede mejorar de forma sustancial si se entienden y ofrecen respuestas a los principales

desafíos que enfrentan y comparten. Este es el propósito central de las recomendaciones mínimas de seguridad digital que presentamos.
Este documento es el resultado del esfuerzo del Laboratorio de Privacidad y Seguridad Digital K+Lab de Karisma, que durante el último año acompañó y aprendió de las personas defensoras del medio ambiente que participaron en este proceso.
Agradecemos a cada una de ellas por permitirnos, a través de sus experiencias, entender sus riesgos y prácticas. Esperamos que este resultado sea un apoyo para el importante trabajo que llevan a cabo.





1. Nota metodológica

Esta primera aproximación a los riesgos y los desafíos que las tecnologías digitales están generando para las personas defensoras del medio ambiente en territorios en conflicto en Colombia se realizó a partir de la experiencia de personas que habitan en tres territorios del país y que forman parte de seis organizaciones cuya misión se centra en el cuidado del medio ambiente. Estas organizaciones aceptaron implicarse en un proceso para que Karisma caracterizara las amenazas digitales que enfrentan y para participar en actividades de capacitación en seguridad digital. Es importante agregar que se realizó un análisis con cada organización con el fin de que tal acción colectiva de análisis de amenazas digitales no representara un riesgo adicional para ellas.

Además de la investigación de escritorio para entender la situación de las personas que defienden el medio ambiente, el trabajo de campo se llevó a cabo con un enfoque cualitativo a través de dos herramientas de investigación y recolección de información: talleres y entrevistas.

Se adelantaron 6 talleres de sensibilización en seguridad digital (con una duración de 12 horas aproximadamente, en cada uno participaron unas 15 personas) y 6 entrevistas a profundidad con líderes y lideresas defensoras del medio ambiente al interior de esas organizaciones. Para referirnos a experiencias concretas, en este documento se usarán citas de entrevistas y experiencias recogidas en los talleres en forma genérica. Se ha hecho un esfuerzo intencional para evitar que los datos en este documento no permitan individualizar a quienes fueron parte del proceso. La ausencia de datos concretos responde entonces a la conciencia sobre los riesgos que tiene esta población y la intención de evitar aumentarlos.

2. Caracterización de las amenazas digitales en contra de las personas defensoras del medio ambiente

Colombia ofrece un entorno hostil en los territorios para quienes luchan por el medio ambiente. Quienes lo hacen deben enfrentarse a diversas amenazas y peligros que van desde la falta de paz que perpetúa la presencia de actores armados -derivada de la violencia política, economías ilegales, migración irregular, minería ilegal y tantos otros fenómenos que atraviesan el país- hasta las decisiones estratégicas del Estado sobre modelos de conservación ambiental y desarrollo económico que crean riesgos y tensiones

entre quienes habitan los territorios[2]. En ese contexto, la intimidación, las amenazas y las violencias directas e indirectas contra las personas defensoras suponen un alto nivel de riesgo que también sucede en los escenarios digitales.
De las actividades realizadas con el grupo de organizaciones defensoras del medio ambiente los siguientes son los riesgos digitales más claros que identificamos:

2.1 Intersección de riesgos digitales y contexto ambiental

Los riesgos digitales no deberían separarse de los contextos ambientales y sociales en los que operan

2. Corte Constitucional de Colombia. (2023). Sentencia SU-546 de 2023: Expedientes T-8.018.193, T-8.136.698, T-8.062.595, T-8.091.278, T-8.242.042, T-8.266.696, T-8.270.692, T-8.365.345, T-8.473.048, T-8.682.067 y T-8.705.913. Acción de tutela instaurada por integrantes de la población líder y defensora de derechos humanos contra la Unidad Nacional de Protección y otros.

las personas defensoras del medio ambiente en América Latina. De hecho, se percibe una relación entre la forma en que se presentan las amenazas y el uso de tecnologías digitales. Situaciones como la vigilancia, el *hackeo*, la intervención de comunicaciones, la exposición de datos personales y el ciberacoso son tácticas que agravan las amenazas físicas y sociales a las que ya están expuestas estas personas[3].

El Acuerdo de Escazú, como el primer tratado regional que incluye disposiciones específicas sobre la protección de defensores ambientales, ofrece un marco crucial para abordar estos riesgos. La Guía de implementación del Acuerdo de Escazú recomienda

3. "CIDH: 2023 cierra con altos índices de violencia contra personas defensoras en las Américas", Comunicado de Prensa, 5 de marzo de 2024. Se puede consultar en https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2024/045.asp#:~:text=Washington%2C%20D.C.%20-%20La%20Comisi%C3%B3n%20Interamericana,al%20menos%20126%20personas%20defensoras

medidas de seguridad holística, que combinan la seguridad física y digital, para proteger eficazmente a los defensores del medio ambiente. Esta guía subraya la importancia de la capacitación en habilidades digitales para mitigar las amenazas y vulnerabilidades en el entorno digital[4].

4. Guía de Implementación del Regional sobre el Acuerdo Regional sobre el Acceso a la Información, la Participación Pública y el Acceso a la Justicia en Asuntos Ambientales en América Latina y el Caribe (Acuerdo de Escazú). Noviembre 11 de 2023. Se puede consultar en https://repositorio.cepal.org/server/api/core/bitstreams/28aa1443-4775-4430-8f15-13a3640bd74f/content De hecho desde la sociedad civil se han venido adelantando esfuerzos para abordar este desafío. Organizaciones como Internews ofrece cursos en seguridad digital para reducir ofrecer herramientas a las personas defensoras del medio ambiente para enfrentar sus vulnerabilidades en el ámbito digital. Se pueden consultar en https://internews.org/blog/internews-lanza-curso-de-seguridad-digital-para-defensores-de-derechos-humanos-y-del-medio-ambiente/

2.2. Amenazas y hostigamientos digitales

Las amenazas virtuales, el hostigamiento en redes sociales y la difamación a través de perfiles falsos son prácticas recurrentes dirigidas contra las personas defensoras del medio ambiente. Estos ataques no solo buscan desacreditar su trabajo, sino también intimidar y silenciar sus voces. La tecnología se utiliza como una herramienta para perpetuar la violencia y la persecución que ya se hace en el mundo físico.

Establecimos con las organizaciones que participaron de la investigación que existe una conexión entre las diferentes formas de violencia: lo que empieza como hostigamiento generalizado e indeterminado en el mundo físico -a través de panfletos y rumores- hacia las organizaciones, se transforma en amenazas en redes sociales y en aplicaciones de mensajería

instantánea -como Telegram o WhatsApp[5]-, que llegan a individualizarse y así el hostigamiento puede materializarse en agresiones físicas que ponen en peligro la seguridad de quienes defienden el medio ambiente. Las amenazas que fueron reportadas a través de redes sociales y mensajería instantánea, pueden caracterizarse como ciberacoso (hostigamiento constante) y doxxing (exposición de datos personales).

Es crucial señalar que de acuerdo con los hallazgos de los talleres y entrevistas, el racismo y el machismo intensifican la agresión dirigida específicamente

5. Telegram o Whatsapp son herramientas de mensajería instantánea, que se diferencian de una red social. Como herramientas de mensajería, su funcionamiento debe compararse a aquel de la correspondencia física, en donde los mensajes que van de un usuario a otro viajan en sobres cerrados, que la compañía no puede abrir y aún si los abriera no podría interpretar. La seguridad, entonces, se convierte en la regla de funcionamiento de esas aplicaciones.

hacia ciertos perfiles de personas defensoras ambientales. "A mí me han golpeado (...) por ser mujer, pues a mi me golpearon" (Entrevista 2), manifestaba una de las defensoras que hizo parte de la investigación. La forma como esto se traslada al entorno digital es algo que deberá explorarse con mayor detalle.

2.3. La exposición de los datos personales facilita el hostigamiento individualizado

Dado que con frecuencia el hostigamiento incluye hacer pública la ubicación y datos de estas personas a través de las redes sociales (*doxing*[6]), se ha aumentado el riesgo de que estos hostigamientos provoquen amenazas y ataques a la integridad física

6. El doxing consiste en recopilar y publicar información personal de alguien o de un grupo, sin su consentimiento, con el objetivo de dañar su trayectoria pública y profesional. Tomado de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-doxing-y-como-podemos-cuidarnos

contra las personas defensoras y sus familias. Sin embargo, en la investigación se estableció que la información personal puede provenir de diferentes fuentes.

Quienes amenazan a estas personas pueden aprovechar información que es pública bien porque la publiquen terceros malintencionados (doxing). porque lo hagan las mismas personas derivada de su presencia en redes sociales, o porque se hace pública ya que la proporcionan en otros espacios y para diferentes trámites -incluso oficiales-. Sobre el último puntor, no puede descartarse que la información personal que aprovechan quienes les amenazan provenga también de información pública resultado de ejercicios de transparencia oficial -como los derivados de los registros de propiedad de vehículos o los de la Cámara de Comercio del lugar- de ciberataques (hackeos) o filtraciones de datos desde entidades públicas o privadas que recibieron esos datos con propósitos legítimos. Esto debe analizarse con mayor profundidad, incluyendo el uso que se pueda dar a estos datos en actividades de vigilancia.

Aunque los espacios físicos como las reuniones y audiencias con la administración pública son espacios en los que pueden ser fácilmente identificadas estas personas, y dónde con frecuencia son amenazadas, quienes participaron en la investigación reportaron que cada vez más las amenazas y hostigamientos pasan a espacios más íntimos como llamadas telefónicas.

Estas personas no solo son más vulnerables a los ataques por actores que les son hostiles, también lo son a ataques de la delincuencia común. Así, por ejemplo, varias personas de las que participaron de la investigación manifestaron haber sido objeto de amenazas telefónicas en las que les exigían dinero para evitar ser agredidas físicamente. Si bien la persona que llamaba se identificaba como parte de un grupo armado, las personas defensoras, como receptoras de estas llamadas, reconocen que en su experiencia esa no es la forma de actuar de estos grupos y por tanto admiten que esto puede ser solo una estafa. Sin embargo, esto no disminuye la zozobra

que las llamadas generan: ellas saben que es algo con lo que deben lidiar y cuyo riesgo se incrementa por la exposición pública de sus datos personales en redes sociales.

2.4. La presencia en redes sociales. ¿Una forma de protección pública o de exposición a la amenaza?

Las tecnologías digitales e internet son herramientas claves de trabajo y protección para quienes defienden el medio ambiente. Es con ellas que pueden explicar, anunciar y aumentar el impacto de sus agendas de trabajo, les permite conectarse con redes más amplias de intereses similares, les ayuda a darse a conocer fuera del territorio, conseguir seguidores y hacer que existan ojos que desde fuera les cuide y reaccionen si algo sucede. De esta forma la presencia en redes sociales puede ser una forma de protegerse, en el territorio, incluso ante la ausencia del Estado. Sin embargo, esa misma herramienta puede aumentar la

vulnerabilidad a ataques físicos y facilitar la vigilancia y el perfilamiento de estas personas por cuenta de los actores que les son hostiles (que pueden provenir del sector privado, público o incluso de la delincuencia común).

Esta dualidad se evidenció en las prácticas de esta población. Internet es una herramienta fundamental para socializar información y ampliar el alcance del trabajo de sus organizaciones. Internet potencia e involucra a nuevos actores al interior de sus comunidades y de otras organizaciones aliadas. En palabras de una de las lideresas: ***"Nuestra consigna es que todo lo hacemos público"*** (Entrevista 1).

Adicionalmente, las organizaciones tienen iniciativas económicas o proyectos comunitarios que los obliga a compartir constantemente información con desconocidos: ***"Cuando me escriben y me piden fotos del lugar a dónde se van a quedar, y de cómo llegar yo tengo que decirles, porque son turistas"*** (Taller de Capacitación Organización 2). En las redes

sociales se publican imágenes y datos para que turistas y personas voluntarias interesadas en conocer los territorios puedan acceder a la información de manera efectiva.

La gestión y las prácticas de seguridad digital en la administración de las redes sociales se hace por parte de las mismas personas defensoras y puede hacerse colectivamente por varias personas de la misma organización. Las prácticas varían considerablemente de organización a organización y se hace de forma más o menos segura. Por ejemplo, una de las lideresas manifestó que, como medida de seguridad y protección de sus datos personales, ***"constantemente estamos cambiando las claves de las redes sociales"*** (Entrevista 3).

Dentro de las situaciones que han vivido las organizaciones mencionaron que han perdido control de sus cuentas de Facebook. Esta situación puede suponer riesgos de filtración de información sensible de la organización y las personas, como lo son las

conversaciones a través de los canales de mensajería de estas plataformas.

La información pública en redes sociales puede ser un riesgo ya que crea espacios de visibilidad que pueden ser utilizados para perfilar, vigilar o atacar a estas personas defensoras. Este es un riesgo que algunas de estas personas reconocen: ***"Yo creo que estoy más expuesto porque lo que yo hablo en mis redes sociales son cosas muy comprometedoras y cosas que son muy importantes a la ausencia del Estado: del abandono, la desaparición de las islas."*** (Entrevista 5).

A pesar de lo anterior, en la investigación comprobamos que las personas defensoras, por lo general, no tienen filtros para compartir información personal en redes sociales, aunque esta sea su ubicación o datos de su vida personal. Tan solo una de las lideresas explicó que ***"lo único que he hecho realmente es que yo no pongo fotos de mis hijos,***

no pongo dónde trabajo (...) tampoco pongo mi teléfono, ni pongo mi dirección” (Entrevista 6). Para ella esta es una medida de seguridad que toma debido a la visibilidad que ha adquirido.

Aunque la difusión de información permite que más personas se enteren de lo que sucede y se unan a sus causas, también puede facilitar su perfilamiento y permitir que actores hostiles la usen en su contra. Es crucial evaluar el riesgo para evitar publicar información crítica o confidencial en redes sociales. Dicha evaluación podría servir para minimizar los riesgos a los que están expuestas.

2.5. Desafíos comunitarios y fragmentación social

La defensa del medio ambiente no sólo genera tensiones con actores externos como empresas, gobiernos o delincuencia común, también provoca divisiones internas dentro de las propias comunidades. Las redes sociales y aplicaciones de

mensajería se utilizan para amplificar estas divisiones, facilitando la desinformación y la manipulación de información que debilita la cohesión comunitaria y aumenta la vulnerabilidad de las personas defensoras del medio ambiente.

Las comunidades no siempre están unidas en la defensa del medio ambiente. Por ejemplo, una propuesta de desarrollo económico a favor de un puerto o una hidroeléctrica puede hacer que mientras unos miembros de la comunidad se posicionan a favor, otros lo hagan en contra. Estas rupturas comunitarias también se han visto potenciadas por el uso de redes sociales. Las personas defensoras indican que las acciones de desprestigio en redes sociales son frecuentes a través de Facebook y grupos de WhatsApp: ***“Todo el tiempo es como una campaña de desacreditación contra nosotros (...) que nosotros queremos engañar a la gente”*** (Entrevista 1). Esto crea rupturas a nivel familiar y comunitario afectando el tejido social de

la comunidad que se trasladan a las redes sociales; internet y los dispositivos tecnológicos se usan como herramientas de amenaza y desprestigio hacia las personas defensoras.

La situación obliga a estas personas a responder y defender la legitimidad de sus procesos de organización constantemente. Incluso sospechan que los ataques pueden provenir de actores al interior de la comunidad, aunque provengan de cuentas con nombres desconocidos, ellos afirman: ***"sospechamos quién puede ser, pero realmente no sabemos quiénes son"*** (Entrevista 1). Esto también sucede en WhatsApp y Telegram donde se conforman grupos para interactuar con la información, y allí las personas defensoras del medio ambiente entran en confrontación directa con las campañas de hostigamiento y de desinformación desde sus cuentas personales.

Mientras quienes los atacan lo hacen con la protección del anonimato, las personas defensoras indican que su legitimidad las obliga a responder desde sus cuentas personales. Esta situación se presenta como una nueva capa de vulnerabilidad que aumenta la exposición de las personas y de su información personal.

En el proceso con las organizaciones y personas que participaron en este estudio, no se determinó si las campañas de desprestigio incluían contenidos desarrollados con herramientas tecnológicas como las *deep fakes*[7]. Dado el creciente uso de estas tecnologías para la desinformación y el desprestigio, analizar su impacto en esta población es algo que podría explorarse con mayor detalle en el futuro.

7. Deep Face son medios audiovisuales manipulados o sintéticos que parecen auténticos y que presentan a personas que parecen decir o hacer algo que nunca han dicho o hecho. Son producidos mediante técnicas de inteligencia artificial, incluidos el aprendizaje automático y el profundo. Tomado de https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

2.6 Mecanismos de coordinación, comunicación y gestión de la información organizacional

Las organizaciones que participaron de la investigación no cuentan con infraestructuras de tecnología para comunicación y gestión de la información propias y separadas de las de las personas que hacen parte de ellas.

Las prácticas de coordinación, comunicación y gestión de las organizaciones no son uniformes, pero se puede indicar que la información de todas las organizaciones se almacena en los computadores personales de sus miembros. Esto no significa que haya un uso colectivo de estos dispositivos; es el computador personal, pero allí es donde queda la información de la organización.

Existen prácticas de cuidado de la información. Por ejemplo, una de las organizaciones intencionalmente

difunde la información no confidencial entre todas las personas miembro con el objetivo de crear copias de respaldo de los documentos, en palabras de la lideresa: ***"Que el día que le suceda algo a mi computador (...) todo mundo tenía la información que yo tenía"*** (Entrevista 4).

En varios casos se estableció que la información se gestiona a través del uso de redes sociales como Facebook e Instagram y aplicaciones de mensajería como WhatsApp y Telegram. Esta información consiste fundamentalmente en conversaciones individuales y colectivas (grupos) y se maneja internamente por la persona que accede a las cuentas de redes. Debido a esta gestión, la información no cuenta con un respaldo más allá del que tienen en los servidores de las empresas que proveen los servicios de redes sociales y mensajería instantánea.

En relación con las prácticas de protección contra el acceso no autorizado a la información, algunas personas al interior de las organizaciones gestionan

la información en computadores con clave, pero la mayoría solo cuenta con teléfonos celulares, muchos de estos sin contraseñas. En estos dispositivos se almacena y gestiona la información a través de aplicaciones como WhatsApp y Facebook.

También se identificó que hay una sensación de desconfianza constante hacia la tecnología digital, lo que confirma que las personas defensoras de derechos humanos en Colombia tienen la percepción de ***"estar chuzadas"***, es decir vigiladas a través de la red celular. Esta percepción ha llevado a una práctica generalizada entre las organizaciones: privilegiar las reuniones presenciales para compartir información sensible. La presencialidad se percibe como una medida de seguridad adicional para garantizar la confidencialidad de las comunicaciones. Así nos lo contó una de las lideresas: ***"Nos reunimos físicamente cuando vamos a tomar decisiones importantes"*** (Entrevista 2).

3. Recomendaciones para el fortalecimiento de la seguridad digital en organizaciones medio ambientales en Colombia

Debido a la penetración de la tecnología digital en la cotidianidad de las personas y su centralidad como herramienta de comunicación y gestión de información para las personas defensoras del medio ambiente, la seguridad digital adquiere una importancia vital en la vida de estas personas en Colombia. Los actores que intentan desarticular sus esfuerzos utilizan estas mismas herramientas digitales para hostigar y perseguir a las personas defensoras.

Desde Karisma consideramos que no se debe escatimar en esfuerzos por salvaguardar la seguridad digital de aquellas personas que trabajan en esta defensa del medio ambiente. Su labor contribuye a la protección de los derechos humanos, la biodiversidad y el equilibrio entre la humanidad y el entorno natural, es con ese propósito que presentamos el siguiente conjunto de recomendaciones básicas de seguridad digital para organizaciones defensoras de medio ambiente en el territorio:

1. Mantener la privacidad de la información que se comparte en redes sociales

Proteger la identidad personal, evitar compartir información personal sensible como dirección, número de teléfono o detalles sobre el trabajo y familia. La información personal siempre debería mantenerse privada y limitar la cantidad de información visible en perfiles públicos.

2. Usar aplicaciones de mensajería instantánea cifradas de extremo a extremo
Con ellas solo el emisor y el receptor del mensaje pueden acceder a la conversación. Recomendamos usar Signal y WhatsApp. Evitar compartir información confidencial en plataformas que no cifren los mensajes, como Telegram en su configuración predeterminada. Adicionalmente, es importante activar la verificación en dos pasos (el mensaje que llega con un código único para ingresar, puede ser un SMS - mensaje de texto - o un código generado por una aplicación de autenticación).

3. Cuidado del phishing y el malware
Para prevenir caer en phishing (robo de información) o en malware (virus) es importante no dar clic en enlaces de fuentes desconocidas o sospechosas, tampoco descargar archivos de esos lugares. Aprender a reconocer señales de phishing en correos electrónicos o mensajes de texto que piden información personal o contraseñas.

4. Fortalecer la seguridad de las cuentas
Fortalecer la seguridad de las cuentas utilizando contraseñas seguras, estas deben ser largas, complejas y únicas para cada uno de tus correos electrónicos y cuentas en redes sociales. Activar la autenticación de dos factores - 2FA - (el mensaje de texto que llega con un código único para ingresar) para agregar una capa adicional de seguridad a sus cuentas. Para no perder las contraseñas, usar un gestor de contraseñas como KeepassXC[8] o Bitwarden[9].

5. Cuida la información que se comparte en línea
Antes de publicar contenido en redes sociales hay que tener cuidado de no publicar información confidencial o comprometedora, por ejemplo

8. https://keepassxc.org/download/

9. En https://bitwarden.com/ se puede descargar la aplicación y acá dejamos una guía para la configuración de la herramienta https://conexo.org/wp-content/uploads/2023/09/1b.-CONF_-Bitwarden-septiembre-2023.pdf

con etiquetas de personas, lugares de encuentro, ubicación en tiempo real, temas de reuniones, etc. Es importante definir el uso y el propósito que tiene cada red social, no todas tienen las mismas funcionalidades y eso es relevante a la hora de publicar y revisar contenido. Para la difusión de información se pueden utilizar boletines cifrados o plataformas seguras para la compartición de documentos, esto evita tener que publicar información crítica directamente en redes sociales.

6. Privacidad en el uso de grupos en la mensajería instantánea

Ser consciente de los riesgos en grupos de WhatsApp y Telegram -que son los que más usa esta población- podría minimizar los riesgos: controlar la configuración de privacidad de los grupos (cerciorarse de quiénes son las personas que hacen parte del grupo), evitar compartir información sensible en grupos donde no todas las personas participantes son de confianza. Adicionalmente, es importante mantener

un grupo más pequeño y controlado para compartir información estratégica y sensible de la organización o colectiva.

7. Respaldar información importante
Realizar copias de seguridad periódicas de la información importante almacenada en el celular, computador, etc y en la nube. Mantener los datos respaldados en lugares seguros (disco duro externo cifrado, usb cifrada) y fuera del alcance de personas no autorizadas. Para copias de seguridad cifradas se puede utilizar Veracrypt[10].

8. Ayuda a mantener espacios seguros en línea
Bloquear y denunciar comportamientos abusivos o amenazantes en plataformas digitales. Es muy

10. Acá puedes descargar https://www.veracrypt.fr/code/VeraCrypt/ y te dejamos esta guía de configuración https://conexo.org/wp-content/uploads/2024/05/8.-CONF_-Cifrado-en-disco-VeraCrypt-BitLocker-FileVault-Abril-2024.pdf

importante mantener registros de cualquier incidente de acoso y, según corresponda, denunciarlo a las autoridades competentes. En https://acoso.online se pueden encontrar recursos que pueden ayudar cuando se presente un incidente.

9. Compartir información con más personas
Compartir conocimientos y mejores prácticas en seguridad digital para fortalecer la seguridad colectiva. Es vital promover la importancia de proteger la privacidad y la información sensible en línea.

4. Conclusión

La seguridad digital es un elemento crucial para proteger la integridad y la labor de las personas defensoras del medio ambiente que, aunque perciben esas amenazas digitales como parte de los riesgos que enfrentan, todavía no han interiorizado cómo éstas no se limitan al ámbito virtual, sino que tienen repercusiones directas en la vida cotidiana y en su bienestar físico y emocional.

Con este propósito desde Karisma creemos que a futuro se deberá continuar este trabajo y proponemos tres prioridades:

1. **Necesidad de capacitación y resiliencia digital:** Es crucial que las organizaciones y las comunidades desarrollen capacidades digitales y estrategias de resiliencia adaptadas a los desafíos actuales. Esto incluye desde la formación en seguridad digital, hasta la promoción de prácticas responsables en el uso de tecnologías de la información y comunicación, fortaleciendo así su capacidad de resistir y responder a los riesgos digitales. Estos procesos deberían estar acompañados de entidades gubernamentales y organizaciones que promuevan la seguridad de las personas que defienden los territorios en Colombia, para garantizar así su defensa y salvaguardar sus vidas.

2. Uso estratégico de las tecnologías digitales: A pesar de los riesgos, las tecnologías de la información también ofrecen oportunidades significativas para la difusión de información y el activismo digital. Las organizaciones pueden utilizar plataformas digitales para visibilizar su trabajo, movilizar apoyo y fortalecer redes de solidaridad local e internacional en torno a la defensa del medio ambiente. Dado que es frecuente que la defensa del medio ambiente recaiga en organizaciones de base comunitaria y ubicadas en entornos rurales, esta responsabilidad está con mucha frecuencia atada a las personas mismas. Es necesario trabajar en mejorar las prácticas y formas de uso de las tecnologías que les permita dar más visibilidad a su labor y mitigar los riesgos derivados de estas tecnologías.

3. Continuar procesos de investigación para comprender los riesgos digitales de estas personas con el fin de mitigar su impacto y garantizar que sigan haciendo su labor: Esta primera aproximación que tuvimos al tema, y que se materializa en este documento, fue útil y da una línea base para mejorar la situación de las personas defensoras del medio ambiente en territorios en conflicto. Sin embargo, establecimos que se debe indagar más sobre otros riesgos que no pudimos profundizar.

Dentro de los temas que se deberían continuar explorando están los siguientes: (a) los que se derivan de que una misma persona no solo sea defensora del medio ambiente sino además pertenezca a otros grupos con riesgos adicionales -como el hecho de ser mujer, parte de la población lgbti o miembro de determinada etnia-; (b) se debería analizar las mejores formas de gestión y transmisión de información

por parte de estas personas, para mejorar esas capacidades en línea con sus prácticas y las herramientas con las que cuentan; (c) sería positivo mantener un constante análisis sobre las conexiones entre la violencia digital y la física, la forma como una se deriva de la otra; (d) es necesario explorar la manera en la que sus datos personales son filtrados y expuestos, incluso en ejercicios de transparencia del sector público o debido a ciberataques o filtraciones de terceros; (e) aunque no se estableció que en estos casos se usen mecanismos sofisticados de desinformación (como deep fakes) en las estrategías de desprestigio, este es un tema que está en amplio crecimiento y por tanto debería ser analizado con mayor detenimiento; (f) la forma como la tecnología puede estar facilitando los procesos de vigilancia por parte de los actores hostiles a esta población, es algo que tampoco fue explorado en esta oportunidad

y que sin embargo también debería ser parte de agendas de investigación a futuro. Finalmente, se requiere analizar la forma como las autoridades encargadas de la protección de las personas defensoras del medio ambiente deben implementar medidas de protección digital en sus programas y rutas de atención.



Fundación
Karisma

<K+LAB>

fundacionkarismaa karismacol @Karisma

karisma.org.co